Environmental Management Consolidated Business Center (EMCBC)

Subject: Cyber Security – Account Management and User Responsibilities

Implementing Procedure APPROVED: ___*(Signature on File)*___
EMCBC Director
ISSUED BY: OFFICE OF INFORMATION RESOURCE MANAGEMENT

1.0 PURPOSE

The purpose of this procedure is to establish the process for managing user accounts, rights, access to special applications, and define users training requirements.

2.0 SCOPE

This procedure is limited to general user access to systems and applications.

3.0 APPLICABILITY

This procedure is applicable to all users accessing EMCBC systems, whether they are directly employed by EMCBC or have need to access EMCBC services or applications.

4.0 REQUIREMENTS

4.1 PL-240-08 Cyber Security – System Security Plan for General Support System

4.1.1 AC-1 Access Control Policy and Procedures
4.1.2 AC-2 Account Management
4.1.3 AC-3 Access Enforcement
4.1.4 AC-5 Separation of Duties
4.1.5 AC-6 Least Privilege
4.1.6 AC-17 Remote Access
4.1.7 AT-1 Security Awareness and Training Policy and Procedures
4.1.8 AT-2 Security Awareness
4.1.9 AT-4 Security Training Records
4.1.10 IA-1 Identification and Authentication Policy and Procedures
4.1.11 IA-2 User Identification and Authentication
4.1.12 IA-4 Identifier Management
4.1.13 IA-5 Authenticator Management
4.1.14 PL-4 Rules of Behavior
4.1.15 PS-1 Personnel Security Policy and Procedures
4.1.16 PS-3 Personnel Screening
4.1.17 PS-4 Personnel Termination
4.1.18 PS-5 Personnel Transfer
4.1.19 PS-7 Third-party Personnel Security
4.1.20 PS-8 Personnel Sanctions

4.1.21 SI-9 Information Input Restrictions

5.0 DEFINITIONS

5.1 SSP: System Security Plan - generated from the EM Program Cyber Security Plan to define all applicable EMCBC cyber security requirements.

5.2 User: Identity of an employee or other individual having a legitimate need to access the EMCBC Domain Network or other EMCBC services through web or remote access protocols.

5.3 Domain Administrator: Individual assigned by the Assistant Director, Information Resource Management (IRM) to control access to the EMCBC domain or other services.

5.4 Application Sponsor: Non-IRM person assigned by their Assistant Director to be the point of contact for application development.

5.5 IRM: Office of Information Resource Management

5.6 Cognizant Assistant Director: Assistant Director who is the controlling subject matter expert for a given application.

5.7 Domain: A single security boundary of one or more computers that form a computer network.

6.0 RESPONSIBILIITIES

6.1 Users: Read, sign, and follow Rules of Behavior.

6.2 Assistant Directors: Approve access to Special Access Rights applications. Notify IRM when user no longer needs access rights.

6.3 IRM: The domain administrators group shall be responsible for:

6.3.1 Create a new user account
6.3.2 Reset a user password
6.3.3 Copy a user account
6.3.4 Move a user account
6.3.5 Disable or enable a user account
6.3.6 Change a user's primary group
6.3.7 Delete a user account
6.3.8 Audit user accounts monthly for rights and access.

7.0 GENERAL INFORMATION

This procedure defines the process by which users are made aware and acknowledge their responsibilities as employees when interfacing with the information system. The procedure

sets requirements for access to EMCBC systems and applications and provides for user indoctrination and training.

8.0 PROCEDURE

Note:

Foreign Nationals: In the event business needs dictate that a specific Foreign National (A Foreign National is a citizen of a nation other than the United States.) be granted access to the EMCBC information system, the AD-IRM will develop a specific plan to address the needs of the organization for the individual in question. No access to the EMCBC network will be provided to a Foreign National without such a plan in place.

8.1 New Users - EMCBC: Upon notification from Human Resources (and verification that the person is not a Foreign National), IRM will establish new user accounts; EMCBC issues accounts to individual users only. User identifiers are provided directly to the individual, not through email. These accounts will be disabled until the start date of the user. A User may be granted access to EMCBC systems prior to their official start date if they are a current government employee and have approval by their Assistant Director. Non-government employees who are identified as having access needs prior to their start date will need approval from both their Assistant Director and the EMCBC Security Officer.

8.1.1 User Agreement: Each user will be given a user agreement (Attachment A, IP-240-01-F1, Rev. 2) that establishes the uses of the EMCBC Information Technology systems. Before the user is granted access, the user will sign and acknowledge that they understand their responsibilities under the agreement. This user agreement allows users General Access to the system. Additional system access may be documented on the user agreement, or by separate agreement. All user agreements will be maintained by IRM.

8.1.2 General Access Rights: All general users are granted access to email, shared drives, individual user drives and access to EMCBC general applications. New Users are given general access rights to EMCBC general applications, such as Correspondence Control and Tracking Systems (CCTS) and Electronic Transit Subsidy Benefit (ETSB), based on their organization permissions by the EMCBC –Intranet and EMCBC Web Based Applications access process. All users have access to the general tools such as Phonebook, Traffic, Forms, Training, Manuals, etc. General Access applications are designated at inception and controlled under configuration management.

8.1.3 Specific Access Rights: Certain applications are limited access due to the sensitivity of their data. These applications require specific permission by the Cognizant Assistant Director for access. These permissions are documented on the User Agreement or a supplemental agreement as user access is changed. All specific access rights are documented on the User Agreement.

8.1.4 Desktop, Laptop Rights and Assignment**:** Each user is issued a desktop or laptop computer for their use. Each system is issued a numbered Asset Tag. This number along with the users name will be updated into system for use with Remote Administration Functions and inventory control. Users will only be granted limited rights on their desktops. Distribution and adding of software will be controlled by System Administrators. Laptop users will be given limited admin rights to accommodate use of the laptop offsite.

8.1.5 Offsite Access: All users are granted offsite access to their email through the use of web-mail. Remote access to data and applications is defined through the users Specific Access Rights. These systems include those required for single and two factor authentication systems. Offsite access is limited to an as needed basis. EMCBC does not allow foreign nationals from sensitive or non- sensitive countries to access EMCBC systems or networks that contain SUI from outside the DOE facility.

8.1.6 Special Software: Certain users may require software that goes beyond that supplied in the Basic DOE Common Operating Environment package. This software is typically Off the Shelf (OTS) software such as Adobe Acrobat, MSProject, Primavera, etc. Such software may be made available with the concurrence of the individuals Assistant Director or Team Leader.

8.2 New Users: Attached Sites: New users at sites that are sub-netted to EMCBC will follow the protocol for EMCBC users. Their access rights will be limited to their portions of the network required to accomplish their job function. The Federal Project Director will sign in lieu of the EMCBC Assistant Director, though access to Specific
Access Applications will require the signature of the Federal Project Director and the Cognizant Assistant Director, including verification that the individual is not a Foreign National.

8.3 Offsite Users: Offsite Users are those users who are not General Access Users under the EMCBC, but require access to specific EMCBC applications in order to coordinate their functions with an EMCBC office. These users are usually at a serviced site or at DOE Headquarters. These users will be given Specific Access Rights without General Access Rights. The offsite user will be required to sign an access form to acknowledge their responsibilities for the sensitivity of the data they are accessing and obtain the permission of the Cognizant Assistant Director for the application they are accessing.

8.4 Vendors: Vendors are given access to the network on as needed basis. Vendors escorted by IRM and not issued general access or an email address are not required to sign a User Agreement. However, Vendors given any long term access allowing for independent access to the Domain will be required to:

8.4.1 Present documentation from their company verifying that they are a U. S. Citizen,

8.4.2 Sign a User Agreement Form.

8.4.2.1 IRM will annotate the User Agreement form with the product the vendor is maintaining and give the document an expiration date a maximum of one year from the nearest current month. The ADIRM may renew the access without generating a new form by annotating the User Agreement.

8.5 Termination of Account and Access**:** Upon notification from HR or the Cognizant Assistant Director, account access will be terminated as required.

8.5.1 General Account Access will be disabled until such time as the disposition of the users' files and emails has been determined. Users leaving EMCBC, but staying in the government service may be allowed access to the email accounts for up 30 days with approval of their Assistant Director. Users leaving government service will be allowed to generate an "Out of Office" email giving out details of their new location and access to their email account will be terminated.

8.5.2 Specific Account Access may be terminated by notification of an Administrator of the application and will be terminated once the employee has left the EMCBC. If the employee has need of the application in his or her new function they may obtain access rights as an Offsite User.

8.6 Account Management**:**

8.6.1 IRM will conduct a monthly audit of General Account Access. Results of the audit will be documented in the IRM log.

8.6.2 IRM will coordinate monthly audits of Specific Access Rights by the Application Sponsor.

8.7 Training**:**

8.7.1 Initial Training: All users will take cyber security awareness training within 30 days of being issued a User ID. Extensions may be granted by the Cognizant Assistant Director with concurrence by the Assistant Director, IRM for extenuating circumstances.

8.7.2 Annual Training: All users will take a cyber security refresher training annually to maintain their access rights to the network. Users may operate up to two months beyond their training due date with the permission of the Assistant Director, IRM.

8.7.3 Updates and Alerts: IRM will periodically issue alerts to identify security issues to the EMCBC users. The purpose of the alerts is to inform the users of

security threats that may affect them in the workplace or at home and are issued at the discretion of IRM.

9.0 RECORDS MAINTENANCE

9.1 Records generated as a result of implementing this document are identified as follows:

9.1.1 User Agreement Form, IP-240-01-F1, Rev. 2

10.0 FORMS USED

10.1 All forms are the latest revision unless otherwise specified.

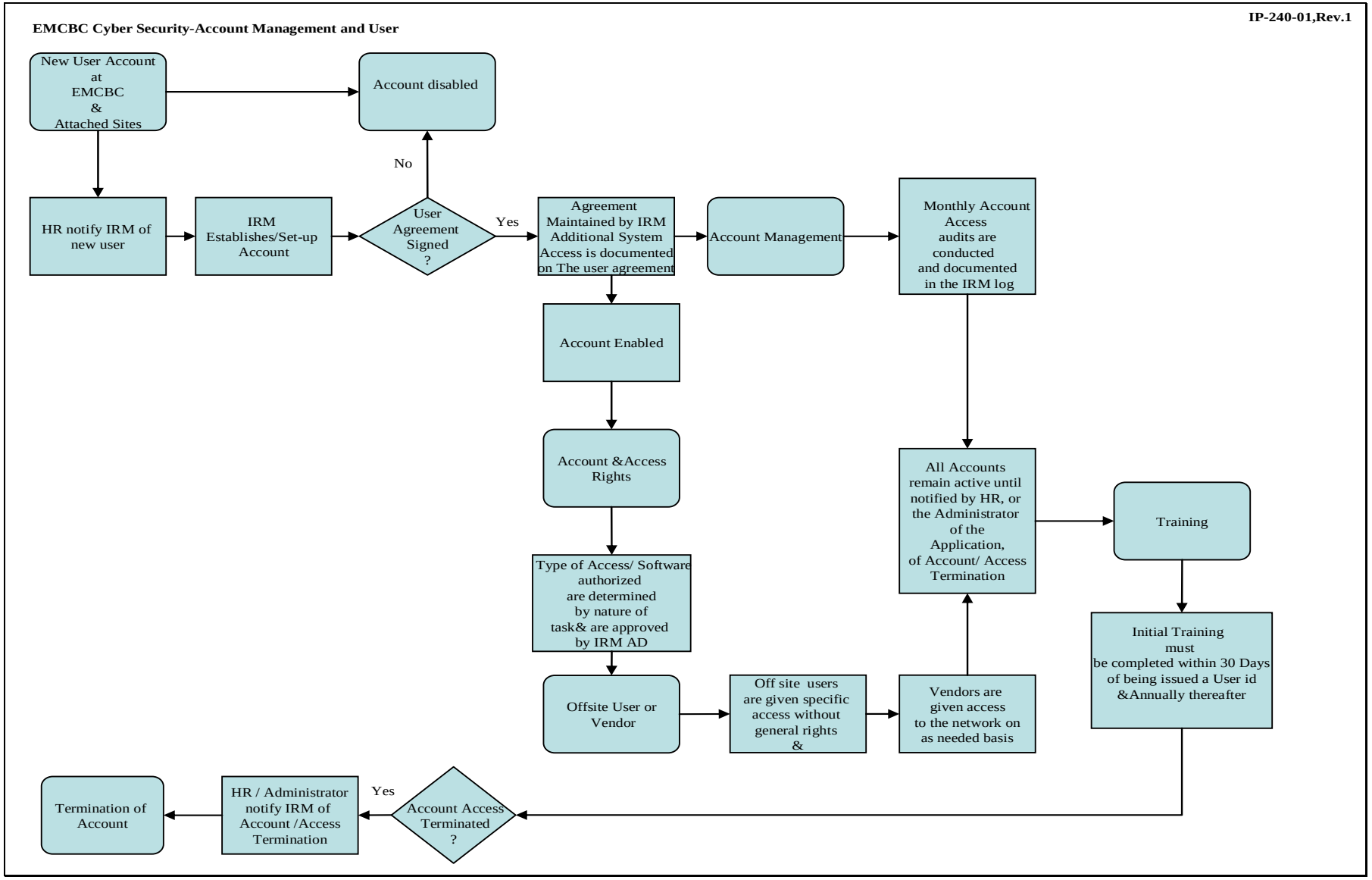
10.1.1 User Agreement Form, IP-240-01-F1, Rev. 2

11.0 ATTACHMENTS

11.1 Attachment A, User Agreement Form, IP-240-01-F1, Rev. 2

11.2 Attachment B, Example of General and Special Access list.

12.0 FLOWCHART



DEPARTMENT OF ENERGY
OFFICE OF ENVIRONMENTAL MANAGEMENT
PROGRAM CYBER SECURITY PLAN
June 16, 2008
RULES OF BEHAVIOR FOR EMCBC COMPUTER SYSTEMS

In compliance with the requirements of OMB Circular A-130, Appendix III, as required by law under the Clinger-Cohen Act, all users of a Government computer system are required to be apprised of the rules that govern the appropriate use of such data processing resources. This applies to both the computer that has been issued to them as well as any computer they are authorized to use apart from what has been issued to them.

To ensure compliance with regulations in this regard, the following conditions of use apply. These conditions form the Rules of Behavior that shall establish evidence of such compliance on an individual basis. As a condition of system access, you are required to read the following and concur at the bottom of this document with a signature by your hand.

1. DOE computers and computer systems are provided for the processing of official U.S. Government information.

2. Accessing Government work files to which I have been given access permission, whether by issued computer or privately owned computer, requires that I abide by the Rules of Behavior described herein.

3. I have no expectation of privacy on any information entered, stored, or transferred through DOE computers, host systems or networks.

4. Use of DOE computers, host systems and networks are restricted to authorized users and I am responsible for all actions taken under my user account or identity.

5. I have attended training and have been instructed on Remote Access security concepts and best practices. If using a privately owned computer to access a Government computer network, I will not circumvent the protections that such access may be subject to.

6. I will use the DOE computer, host system and network only as authorized. I understand that I am permitted to use this system for limited personal use as described in the appropriate use policy elements that I have reviewed.

7. If I have been authorized to process classified information, I will not enter classified data into a classified system if that data is of a higher classification level than the system is authorized to process.

8. Under no circumstances will I ever enter classified data into an unclassified system or permit anyone to do so. If I do so accidentally or otherwise receive by email or acquire such information unexpectedly from anyone, I will immediately notify my supervisor.

9. If I observe anything that indicated inadequate security, misuse of this system or virus infection, I will immediately notify my supervisor.

10. I will follow office security procedures, official regulations, and policies applicable to computer systems operation, to include applicable password policy.

11. I will not use any DOE computer and/or the host system to gain unauthorized access, or attempt to gain unauthorized access, to other computers or computer systems. Further, I will not use any DOE computer and/or the host system to launch denial of service, or attempt to launch denial of service, attacks against other computers or computer systems.

12. I understand that the host system and network is monitored to ensure information security, system integrity, and the limitation of use for official purposes. By using the host system and network, I am expressly consenting to such monitoring and agree that any and all information derived from such monitoring, including connection logs between computers and my subscriber information may be used as a basis for administrative, disciplinary, or criminal proceedings.

13. I understand that my supervisor may instruct me to reduce my level of personal usage based on monitoring reports of such activity.

14. I also hereby consent to the opening of any stored filed and/or electronic mail that may be stored either on the host system or on any DOE computer workstation by my supervisor, chain of command or any individual duly authorized under color of law. If such information has been encrypted by me, I shall freely provide the means of decryption to provide such access.

15. I hereby expressly authorize the system administrator to provide my supervisors and law enforcement personnel with any and all information pertaining to my alleged misuse and abuse of any DOE computer and/or the host system and/or network.

16. I further certify that I am not a Foreign National

17. I have been provided a copy of this Agreement and understand that the system administrator will maintain the original.

18. I certify that I will follow all requirements for the protection of sensitive data such as Personally Identifiable Information, Sensitive Agency Information, Source Selections Information, etc.

19. I understand that he following activities on DOE computer resources are prohibited and constitute misuse or abuse and can lead to discipline up to removal:
    a. Activities that include, but not limited to hate language; material that ridicules others on the basis of race, creed, religion, sex, disability, national origin, or sexual orientation; and harassment or threats.
    b. The creation, downloading, viewing, storage, copying or transmission of sexually explicit or sexually oriented materials.
    c. Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services) with which an employee is associated.
    d. Any personal use of government resources that may mislead someone into believing that the employee is acting in an official capacity.
    e. Engaging in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
    f. The above inappropriate activities are not all inclusive and employees must abide by DOE directives on appropriate use of computer systems.
    g. Employees will not disseminate government e-mail addresses on flyers, personal business publications, Internet websites or anything that would cause significant increase in the number of e-mail messages received.

Levels of Access:

Access Authorized for General Use, as defined by the General Use Access Protocol.

	User's Signature	Date:
	Printed Name	
	Organization	

Attachment A
Page 4 – 4

Additional Specific Access Rights granted to EMCBC Systems and Applications:

SYS/APPLICATION	ACCESS TYPE	DATA SENSITIVITY	A. D. APPROVAL

NAME	
ORG	

Attachment B

EMCBC Intranet Developed Applications and Links	Special Access Rights
Blackberries, Cell Phones	
CCTS (Controlled Correspondence Tracking System)	
CDA (Congressionally Directed Activities)	x
Dictionary/Thesaurus	
DOE Acronyms	
DOENet Sites	
E-Clps	X
ECP (Employee Concerns Program)	X
EEOICPA Database	X
ETSB (Electronic Transit Subsity Benefit)	
FOIA Database	X
Forms	
Help Desk Requests	
IM Maintenance Log	
Manuals	
MS Project Viewer	
Pcard	X
Pegasus	X
Phonebook	
Policies, Procedures & Plans	
Printer Management	
Purchasing	
REDS (Real Estate)	x
RIF (Reduction in Workforce)	x
Site Profiles	
Traffic	
Training	

EMCBC RECORD OF REVISION

DOCUMENT

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

- Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.
- Placing the words GENERAL REVISION at the beginning of the test.

Rev. No.	Description of Changes	Revision on Pages	Date
1	Original Procedure	Entire Document	1/22/07
2	Updated references	1	6/16/08
2	Spelled out SSP	2	6/16/08
2	Clarified Foreign Nationals cannot get accounts	3, 9	6/16/08
2	Changed date of Attachment A	8	6/16/08

CONTROLLED DOCUMENT CHANGE REQUEST

DATE: ____6/2/2008_____

INITIATOR: ____W. Best _____

INITIATOR PHONE NUMBER: _60530_____

DOCUMENT AFFECTED: _____

SECTION: 4.1 5.1 8.0_____ PARAGRAPH #:_____

CONTROLLED NUMBER : IP-240-01_____ PARAGRAPH #:_____

NEW CONTROLLED NUMBER: IP-240-01,Rev.2

PROPOSED
REVISION: _____Section 4.1, added new references to new SSP, 5.1 clarified SSP definition, Section 8.0 Explicitly stated that no Foreign Nationals may have access unless the AD-IRM creates a specific plan to address. IP-240-01-F1, Users must confirm they are not foreign nationals

JUSTIFICATION: Revising to align with cyber security requirements_____

Requested by:
___W. Best _____ Date_06/02/08_____

Approval:
_____ DATE: _____
Associate Director

Assigned to: _____ DUE DATE: _____

IP-250-01-F2, Rev.1

Document Review Record Sheet				
Document Title	Cyber Security – Account Management and User Responsibilities			
Control Number	Revision No. 2	Date Issued for Review 06/02/2008		
The subject document is being submitted for your review, approval or comments. Since this review is controlled, a response is required from all reviewers. Therefore, please return the review sheet with or without comments				
To: L. Chafin	Extension: 60461	By: 06/16/2008		
Additional Instructions:				
Reviewer	Approve	Approve w/Comments	Do Not Approve	Signature of Reviewer
B. Fain				
M. Roy				
W. Best				
L. Schlag				
H. Taylor				
R. Holland				
T. Brennan				
R. Everson				
T. J. Jackson				
J. Craig				
Comments may be attached to a separate sheet of paper				
APPROVE: Signifies the reviewer's acceptance of the document issued for review.				
APPROVE w/comments: Signifies the reviewer's overall acceptance of the document regarding concept, practice, implementation, provisions and assigned responsibilities. However, the reviewer has suggestions as to the organization of its contents or helpful additions and/or deletions. These comments are termed "non-mandatory comments" and do not require formal resolution between the reviewer and preparer.				
DO NOT APPROVE: Signifies that the reviewer has identified significant problems regarding concept, practice, implementation or responsibilities that render the document unacceptable and/or not in conformance with stated requirements. Such problem areas must be clearly identified by the reviewer. It is mandatory for the preparer to resolve these comments with the reviewer document the resolution and obtain the reviewers concurrence for the resolution. The reviewer's written concurrence with the resultant change in disposition shall be documented on this form.				
General Review Comments:				
When review is delegated, the designated reviewer shall review and indicate concurrence with the designee's review comments and recommend disposition:				
Designated Reviewer	Concur	Do Not Concur	Signature	Date

IP-251-01-F3, Rev.1